REMARKS

Claims 21-23, 25, 26 and 29-43 are currently pending in this patent application as a result of the preliminary amendment that was filed with the application papers.

No claims are presently indicated as being allowable. More specifically, the Examiner has rejected claims 21, 22, 25, 26, 29, 30 and 32-39 under 35 USC 102(e) as being anticipated by Chen et al. (US 2004/0233910 A1). The Examiner has rejected claims 23 and 31 under 35 USC 103(a) as being unpatentable over Chen et al. in view of Rabe et al. (US 7,194,538). The Examiner has rejected claims 40-43 under 35 USC 102(b) as being anticipated by Iwatani (US 2001/0054093 A1). These rejections are respectfully disagreed with, and are traversed below.

Claim 1 recites in part:

> managing the SAN by a SAN Management software with at least a SAN Management server and at least a SAN Management client with a communication path to said Fibre Channel Adapter,
> **separating requests issued by the SAN Management server into at least two groups,**
> **a first group is processed by the Fibre Channel adapter and the SAN on behalf of the SM Management client** in place of operating system images which share the same Fibre Channel Adapter, corresponding to a trusted path, and
> **a second group is processed by the operating system images** without the need to send or receive requests to or from the Fibre Channel adapter and the SAN.

The disclosure of Chen et al. is directed to a different type of SAN architecture than that disclosed and claimed in this patent application. This is made evident at least in the following ways.

The Examiner states that the claimed element "separating requests issued by the SAN Management server into at least two groups" is anticipated by Figures 5 and 6. The Examiner also equates the "SAN Management server" with the storage server 240 of Chen et al., and the SAN Management client with one of the client computers 210 of Chen et al. That is, as

interpreted by the Examiner each client computer 210, containing both SAN 205 and NAS 215 blocks, functions as the SAN Management client.

It is instructive to also review Figure 4 of Chen et al. and the corresponding portions of the specification at paragraphs [0040] to [0056] when considering the flow diagrams of Figures 5 and 6. More specifically, paragraph [0059] of Chen, specifically noted by the Examiner, states:

> Once a generic storage-related request is generated, it is sent to SAN/IP driver 445a. In step 555, **SAN/IP driver 445a asks whether the client is verified and authenticated and connected to storage server 240. If not, step 560 verifies and authenticates the client and connects to storage server 240. Once the client is verified, authenticated, and connected, step 565 enhances the reliability of the UDP protocol and transmits the generic storage-related request via RPC to storage server 240.** After storage server 240 acts on the request as described in the flowchart of FIG. 6, the completed results and/or responses are received by SAN/IP driver 445a from storage server 240 in step 570. The response is sent back to SAN SCSI driver 440 which, in step 575, translates or formats appropriately the received results/responses, and returns the response to operating system 420 in step 595.

Paragraph [0060], also noted by the Examiner, states:

> FIG. 6 describes the storage server's operations. In step 610, **SAN/IP driver 445b in storage server 240 receives the generic storage-related request.** In step 615, SAN/IP driver 445b attempts to verify and authenticate the request. In step 620, I/O core virtualization layer 490 takes over and asks if the verification succeeded. If so, step 625 converts the generic storage-related request to a generic storage-related command. Step 630 then asks whether the generic storage-related command requires access to a device for completion. The answer to this is yes if the generic storage-related command is one such as a Read or a Write. If the generic storage-related command is one such as Ready, Identify, or Capacity, which does not need device access to complete, step 635 produces the appropriate results and/or responses and packages the results into a generic storage-related reply. A generic storage-related reply is also generated if the verification/authentication in step 620 failed. Step 695 then transmits this generic storage-related reply back to the client that sent the request.

Clearly, **these paragraphs do not expressly disclose or suggest** at least the claimed element of

"separating **requests issued by the SAN Management server** into at least two groups". Figure 5 (and paragraph [0059] describes **operations that occur at the SAN clients 205** (or NAS 215).

Reference in this regard can be made to paragraph [0035], where Chen et al. state:

> As illustrated in FIG. 2A, one embodiment of the SAN of the present invention consists of one or more client computers 210, each able to act as both a SAN client 205 and a NAS client 215, connected to a computer network 200, such as a LAN, MAN, or WAN, a storage manager 280, one or more storage servers 240, and storage devices 250. (In the description of FIGS. 1A and 1B, SAN client computers 110 were called "servers." In the description of embodiments of the invention as shown in FIG. 2A and later figures, computers 210, although technically "servers" within the LAN, MAN, or WAN, are "clients" of storage server 240 and will be referred to as such.)

As such, **Figure 5 <u>does not disclose</u>** "separating requests issued by the SAN Management server into at least two groups", **but instead describes the processing of a request block generated at one of the client computers (SAN <u>client</u> of storage server 240),** and the determination of whether the associated command is a local command or a remote command. If it is a remote command, it is converted to a generic command and sent to the storage server 240 (called the SAN Management server by the Examiner) for execution. Paragraph [0060] and Figure 6 merely disclose how the received generic command is processed at the storage server 240.

It should also thus be clear that there is no express disclosure in Chen et al. of at least the last two elements of claim 21.

It should be readily apparent that Chen et al. do not anticipate claim 21, and that claim 21 should be found to be allowable over Chen et al. The same argument is advanced for the somewhat similar computer program product claim 29.

In that claims 21 and 29 are allowable over Chen et al., then all claims that depend from claims 21 and 29 should also be found to be allowable, whether considered only with Chen et al. or with Chen et al. in view of Rabe et al.

Further in this regard, and considering for example claims 22, 25 and 26, it is not seen where paragraph [0055] of Chen et al. anticipates, as in claim 22, "routing all information contained in unsolicited messages generated in the SAN and Fibre Channel adapter to the SAN Management server by the SAN management client"; where paragraph [0055] of Chen et al. anticipates, as in claim 25, "accessing all information relevant for billing individual operating system images generated in the Fibre Channel adapter and SAN only through the SAN Management client on the trusted path"; or where paragraph [0044] of Chen et al. anticipates, as in claim 26:

> "said SAN Management server providing authorization data to the SAN Management client to execute requests from said first group, and said SAN Management server and SAN Management client providing authorization data to the OS images to execute requests from said second group, and operating the OS images so that they are only enabled to execute a limited command set in the SAN".

Paragraph [0044] appears to simply discuss the operation of the application 410 and operating system 420 at the client computer. There is no express disclosure of, nor any suggestion of, the subject matter claimed in claim 26.

Turning now to the rejection of claims 40-43 as being anticipated by Iwatani, the disclosure of Iwatani has been carefully reviewed, and it is not seen where Iwatani expressly discloses the claimed subject matter.

For example, claim 40 includes a recitation that s SAN Management server includes:

> a first interface to couple to a SAN Management client that comprises a trusted operating system (OS), said SAN Management client being coupled to a SAN via a SAN adapter; and
>
> a second interface to couple to at least one untrusted operating system, said at least one untrusted OS being coupled to the SAN via the SAN adapter and via a unit for regulating access to the SAN;
>
> where said SAN Management server comprises logic for distinguishing a first set of requests from a second set of requests, where the first set of requests are

processed in cooperation only with said SAN Management client, and where the second set of requests are processed at least in part by the at least one untrusted operating system.

Paragraph [0055] of Iwatani, cited by the Examiner with regard to the first two elements of claim 40, states only:

> The system administrator sets up the region on the storage side that attempts to access the SAN integrated management mechanism 500 from the host side and the FCA (fiber channel adapter) and the HBA (host bus adapter) that are used when accessing that storage. These settings are referred to as the access path settings.

Clarification is respectfully requested as to how paragraph [0055] expressly discloses the subject mater claimed in the first two elements of claim 40.

Paragraphs [0060] to [0066] appear to describe log-in sequences, setting up access settings and access control by the fibre channel adapter based on WWN (worldwide name) and PID (port identification). Clarification is respectfully requested as to how paragraphs [0060]-[0066] expressly disclose the subject mater claimed in the last element of claim 40 (i.e., "said SAN Management server comprises logic for distinguishing a first set of requests from a second set of requests, where the first set of requests are processed in cooperation only with said SAN Management client, and where the second set of requests are processed at least in part by the at least one untrusted operating system").

Absent such a showing, claim 40 should be found to be allowable over Iwatani, as should claim 41 that depends therefrom. Further in this regard, claim 41 recites: "where said first set of requests comprise at least one of a SAN request and a SAN adapter request, and said second set of requests comprise a request for untrusted OS configuration data."

Paragraphs [0065] and [0066] of Iwatani state only:

> Here, the FCA determines whether or not access is permitted of the destination

information of the WWN or PID that has been secured. The processing will continue only for devices permitted access. Access attempts by those without permission will result in check condition or other error responses.

There are some devices that have no SAN management mechanism among the host devices making up the SAN. There are also devices which do not provide the aforementioned host affinity function even inside the storage device. For this reason, the management mechanism 500 would not designate the access relationships for this sort of device, but the security would be assured by other security systems (such as Storage affinity or zoning).

Clarification is respectfully requested as to where these two paragraphs expressly disclose "said second set of requests comprise a request for untrusted OS configuration data."

Claims 42 and 43 are also not anticipated by Iwatani, at least for the reason that claim 42 recites in part:

said SAN Management client comprising logic for processing a first set of requests identified by the SAN Management server in cooperation only with said SAN Management server, where a second set of requests identified by the SAN Management server are processed at least in part by the at least one untrusted OS;

where said first set of requests comprise at least one of a SAN request and a SAN adapter request, where said second set of requests comprise a request for untrusted OS configuration data.

The Examiner, in rejecting claim 42, refers again to paragraphs [0060] to [0066]. However, and as was noted above, these paragraphs appear to simply describe log-in sequences, setting up access settings and access control by the fibre channel adapter based on WWN and PID. Clarification is respectfully requested as to how paragraphs [0060]-[0066] expressly disclose the subject mater claimed in the last two elements of claim 42. Absent such a showing, claim 42 should be found to be allowable over Iwatani, as should claim 43 that depends therefrom.

The Examiner is respectfully reminded that for a rejection to be made on the basis of anticipation it is well recognized that "to constitute an anticipation, all material elements recited in a claim must be found in one unit of prior art", Ex Parte Gould, BPAI, 6 USPQ 2d, 1680, 1682 (1987),

citing with approval <u>In re Marshall</u>, 578 F.2d 301, 304, 198 USPQ 344, 346 (CCPA 1978).

It has been clearly shown above that not all material elements of at least the independent claims are found in the disclosures of Chen et al. and Iwatani. As such, the rejections made under 35 USC 102(e) and 102(b) are inappropriate and should be withdrawn.

A favorable reconsideration that results in the early allowance of all of the pending claims is earnestly solicited.

Respectfully submitted:
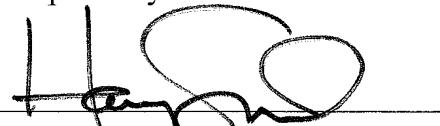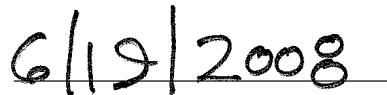
_____   6/13/2008
Harry F. Smith   Date

Reg. No.: 32,493

Customer No.: **49132**

HARRINGTON & SMITH, PC

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400   Facsimile: (203)944-0245

email: hsmith@hspatent.com

Filed electronically